IN THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA	)	Case No.: 3:18MJ5056
	)	
v.	)	**Filed Under Seal**
	)	
The Domain Name COINGATHER.COM	)	
	)	

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANTS

I, Danny Cook, Task Force Officer (TFO) of the Federal Bureau of Investigation (FBI), being duly sworn, hereby declare as follows:

INTRODUCTION

1. I am a Task Force Officer (TFO) with United States Federal Bureau of Investigation (FBI). I am currently assigned to the FBI cyber squad within the Detroit Division that investigates cyber crime, to include matters related to computer intrusion (i.e. “hacking”), fraud and related activity in connection with access devices and fraud perpetrated over the Internet. In addition to the FBI, my training includes over 18 years with the Michigan State Police (MSP), which encompasses my time with the MSP Computer Crimes Unit (CCU) and the Michigan Cyber Command Center (MC3).

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set

forth all of my knowledge about this matter.

3. As set forth below, there is probable cause to believe that the Subject Domain Name, COINGATHER.COM, is property used, or intended to be used, to commit or facilitate violations of Title 18, United States Code, Section 1960 (Prohibition of unlicensed money transmitting businesses), and subject to seizure and forfeiture pursuant to 18 U.S.C. §§ 981 and 982. I make this affidavit for a warrant to seize the property described in Attachment A, specifically, the Subject Domain Name, COINGATHER.COM.

4. The procedure by which the government will seize the Domain Name is described in Attachment A hereto and below.

BACKGROUND ON VIRTUAL CURRENCY AND DOMAIN NAMES

5. Based on my training and experience and information learned from others, I am aware of the following:

Virtual Currency

6. Virtual currency is a type of electronic asset that is circulated over the Internet as a form of value. Bitcoin is one common variety of virtual currency. Bitcoin, like many other types of virtual currency, is not issued by any government, bank, or company, but rather is controlled through computer software operating via a decentralized, peer-to-peer network.

7. To acquire virtual currency, a typical user will purchase it from a virtual currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollar, Russian ruble, €). When a user wishes to purchase virtual currency from an exchange, the user will customarily send payment in the form of fiat currency, often via bank wire, or other virtual currency to an exchange, for the corresponding quantity of virtual currency, based on a

fluctuating exchange rate. The exchange, usually for a commission, will then either sell the user virtual currency from the exchange's reserves or will attempt to broker the purchase with another user who is trying to sell virtual currency. The purchased units of virtual currency are then transferred to the purchaser, allowing the user to conduct transactions with other virtual currency users. Exchanges may also allow users to exchange one form of virtual currency for another. Each exchange option (i.e., U.S. Dollar to bitcoin, bitcoin to litecoin, litecoin to Euros) is commonly called a "currency pair."

8. Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act (BSA) and must take a variety of steps to prevent money laundering.[1] Title 31, United States Code, Section 5330 and Title 31, Code of Federal Regulations, § 1022.380(a) provides, in relevant part, that any money services business (MSB) must register with the Financial Crimes Enforcement Network (FinCEN). In a heavily publicized guidance issued on March 18, 2013, FinCEN confirmed the applicability of its MSB regulations specifically to virtual currency exchangers. Title 18, United States Code, Section 1960, criminalizes the operation of an unlicensed MSB.

<u>Domain Names</u>

9. <u>Internet Protocol Address</u>: An Internet Protocol address (IP address) is a unique

[1] Virtual currency exchanges as defined here are "money transmitters" as defined at 31 C.F.R § 1010.100(ff)(5) and "financial institutions" as defined at 31 C.F.R § 1010.100(t). The BSA and its implementing regulations require an MSB to develop, implement, and maintain an effective written anti-money laundering (AML) program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. Virtual currency exchanges are therefore required to implement a written AML program that, at a minimum: (a) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance; (b) designates an individual responsible to assure day to day compliance with the program and BSA requirements; (c) provides training for appropriate personnel, including training in the detection of suspicious transactions; and (d) provides for independent review to monitor and maintain an adequate program. 31 U.S.C. §§ 5318(a)(2) and (h)(1); 31 C.F.R. §§ 1022.210(c) and (d).

numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs.

10. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, “usdoj.gov” and “cnn.com” are domain names.

11. Domain Name System: The domain name system (“DNS”) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or “labels,” that are delimited by periods, such as “www.example.com.” The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the “top-level” domain. For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, the “example” second-level domain, and is the web server.

12. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into Internet Protocol (“IP”) addresses.

13. Registry: For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. For

example, the registry for the ".com" and ".net" top-level domains are VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

14. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a "registrant." Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address a particular IP address resolves through an online interface. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

15. Whois: A "Whois" search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0- 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0- 12.345.67.99.

CASE BACKGROUND

16. Since 2015, the FBI has been investigating an intrusion into a Michigan-based virtual currency exchange (hereinafter, "Victim Company 1") in which virtual currency was stolen. Over the course of that investigation, law enforcement identified David Bushea (hereinafter, "the CoinGather administrator") as an individual associated with the stolen funds.

On November 17, 2017, the Honorable Magistrate Judge James R. Knepp II issued a warrant in the Northern District of Ohio for a search of the CoinGather administrator's residence for evidence related to the intrusion and theft from Victim Company 1. During the execution of the search, law enforcement observed evidence of violations of 18 U.S.C. § 1960 – specifically, the operation of a virtual currency exchange called "CoinGather."

17. The CoinGather administrator was interviewed at his residence on November 21, 2017, and admitted to running CoinGather, an unlicensed virtual currency exchange. The CoinGather administrator informed law enforcement that he was the sole administrator of CoinGather. The CoinGather administrator advised that he hosted the CoinGather exchange on a computer server located at his employer's premises. He indicated that he established a direct connection from his residence to his employer's server, and that his employer was not aware of the connection. He further advised that the virtual currency wallets associated with CoinGather were stored in Virtual Machines (VMs) on those servers, and that computers in his garage were the primary system used to manage the virtual currencies associated with CoinGather.

18. During the search of the CoinGather administrator's residence, FBI personnel located computers in the CoinGather administrator's garage. FBI personnel determined that the machines were logged into the CoinGather administrator's employer's servers, with administrative access to virtual machines.

COINGATHER EXCHANGE BACKGROUND

19. Based on historic open-source research, including a review of archived web pages, and information provided by the CoinGather administrator, CoinGather was a virtual currency exchange that launched in 2014. CoinGather allowed users to buy and sell virtual currencies, and to transfer virtual currencies to other CoinGather users. Users could readily

create free accounts on CoinGather's website, COINGATHER.COM (the Subject Domain Name). CoinGather did not require users to supply verified identity documentation.

20. As of August 1, 2017, CoinGather supported trading of over 60 currency pairs, including trades involving Bitcoin, Litecoin, Megacoin, PutinCoin, and many others. CoinGather supported only virtual currency to virtual currency exchange; the platform did not support any fiat currency conversion. CoinGather allowed users to vote on what new virtual currencies they wanted added to the platform.

21. CoinGather collected a commission on each purchase and sale of virtual currency conducted on COINGATHER.COM. CoinGather charged 0.25% for both buy and sell orders. CoinGather also charged withdrawal fees, ranging from 0.1% to 1%, depending on the virtual currency.

22. CoinGather communicated with customers through an official Twitter account, as well as through an account on BitcoinTalk.org, a popular message board focused on virtual currency. According to a message posted on CoinGather's official Twitter account, the site purported to have had over 16,300 orders placed on the exchange as of May 5, 2016.

23. Based on an online review of the Financial Crime Enforcement Network ("FinCEN") Money Services Business (MSB) registration website,[2] I have confirmed that CoinGather was not registered with FinCEN as an MSB. According to a query of the Ohio Secretary of State website conducted by FBI personnel, there are no records, registration, or licensing associated with CoinGather or the CoinGather administrator. This lack of registration occurred despite CoinGather's operation as a virtual currency exchange.

[2] FinCEN's MSB Registrant webpage contains entities that have registered as Money Services Businesses pursuant to the Bank Secrecy Act regulations at 31 CFR 1022.380(a)(f).

THE COINGATHER.COM DOMAIN

24. CoinGather's business was conducted through the Subject Domain Name, COINGATHER.COM.

25. A search of publicly available WHOIS domain name registration records revealed that the COINGATHER.COM Domain was registered on or about September 24, 2012 through the registrar GoDaddy.com, LLC, which has its headquarters at 14455 N. Hayden Road, Suite 219, Scottsdale, Arizona 85260. The publicly available WHOIS database lists the registrant of the domain COINGATHER.COM as Registrant Private at Domains By Proxy, LLC. Domains by Proxy, LLC is an entity that allows website owners to keep their contact details private during the domain name registration process.

26. Publicly available WHOIS records also identified CloudFlare, Inc.[3] as a point through which web traffic for the Subject Domain Name was routed.

27. The top-level domain for the Subject Domain Name is Verisign. Verisign currently manages all .com, .net, .cc, .name, and .tv domains.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

28. Title 18, United States Code, Section 981(a)(1)(A) provides, in relevant part, that any property involved in a transaction or attempted transaction in violation of the prohibition of unlicensed money transmitting business (18 U.S.C. § 1960) is subject to civil forfeiture to the United States government.

29. Title 18, United States Code, Section 981(b) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United

[3] Cloudflare, Inc., is a U.S. based company headquartered in San Francisco, California that provides content delivery network and Internet security services.

States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

30. Title 18, United States Code, Section 982(a)(1) provides, in relevant part, that any property involved in a transaction or attempted transaction in violation of the prohibition of unlicensed money transmitting business (18 U.S.C. § 1960) is subject to criminal forfeiture to the United States government.

31. Title 18, United States Code, Section 982(b)(1) authorizes the issuance of a criminal seizure warrant under Title 21, United States Code, Section 853(f) which provides in relevant part that a seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture.

32. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the Subject Domain Names for forfeiture. By seizing the Subject Domain Names and redirecting it to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the Subject Domain Names will prevent third parties from continuing to access the COINGATHER.COM websites in their present form.

33. Title 18, United States Code, Section 981(h) provides that venue for civil forfeitures brought under this section lies in the district either where the defendant owning the property is located or in the judicial district where the criminal prosecution is brought.

34. Title 21, United States Code, Section 853(j) provides that venue for criminal forfeitures brought under this section lies in the district where the defendant owning the criminal forfeiture is located or in the judicial district where the criminal prosecution is brought.

35. As set forth above, there is probable cause to believe that the Subject Domain Name is subject to civil and criminal forfeiture because it was used in the commission of violations of 18 U.S.C. § 1960 (Prohibition of unlicensed money transmitting businesses). Specifically, the CoinGather.com domain was involved in – and enabled – CoinGather's exchange activity and transactions, which were conducted in violation of 18 U.S.C. § 1960.

SEIZURE PROCEDURE

36. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the ".com" top-level domain, Verisign, Inc., headquartered at 12061 Bluemont Way, Reston, Virginia ("Verisign"), shall be directed to restrain and lock the Subject Domain Name pending transfer of all right, title, and interest in the Subject Domain Names to the United States upon completion of forfeiture proceedings, to ensure that changes to the Subject Domain Names cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI or DOJ.

37. In addition, upon seizure of the Subject Domain Name by FBI, Verisign will be directed to associate the Subject Domain Names to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the Subject Domain Name will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

CONCLUSION

38. Based on the information contained in this affidavit there is probable cause to

believe that the Subject Domain Name is property that has been used, or is intended to be used, to commit or facilitate criminal violations of 18 U.S.C. § 1960 (Prohibition of unlicensed money transmitting businesses).

39. Accordingly, the Subject Domain Name is subject to civil and criminal forfeiture and seizure pursuant to 18 U.S.C. §§ 981 and 982.

Accordingly, it is requested that a seizure warrant be issued for the Subject Domain Name, COINGATHER.COM.

FURTHER THIS AFFIANT SAYETH NOT.

Danny Cook
Task Force Officer
Federal Bureau of Investigation

Mar 6, 2018

Sworn to via telephone after
submission by reliable electronic
means. Crim.Rules. 4.1; 41(d)(3)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

James R. Knepp, II
United States Magistrate Judge